

### **REMARKS**

The final Office Action dated 2 April 2007 has been received and its contents carefully studied. Claims 1-57 and 60-67 are pending. The independent claims are claims 1, 29, 30, 60, 65, and 66. All claims now stand rejected based on new grounds of rejection.

In the previous Office Action, claim 1 was rejected as anticipated under 35 U.S.C. § 102(b) by *Hayashi Seiichiro* (JP 09-261218). Claim 24 was rejected as obvious from *Seiichiro* in view of *Hurtado* (U.S. Patent No. 6,418,421). Applicant then amended claim 1 to include the elements of claim 24, which dealt with “usage limitation s”, and Applicant also amended claim 1 to include material from page 13 of the application (stating that one of the usage limitations must be a temporal limit).

Now, claim 1 is rejected as obvious under 35 U.S.C. § 103(a) from *Seiichiro* in view of a new reference: *Abburi et al.* (USPG PUBs 2003/0084306 A1). Independent claims 29, 30, and 65 are now rejected on the same grounds. Independent claims 60 and 66 are now rejected as obvious under 35 U.S.C. § 103(a) from *Seiichiro* and *Abburi* in further view of another new reference: *Lauper et al.* (U.S. Patent No. 7,016,666). *Lauper* is cited for the storage module of claim 66.

### **Summary of the Present Invention**

The present invention includes a method allowing user identification or data encryption with a public key technique, for a user who already has a certificate and corresponding secret key for signatures using another system. For example, a temporary key can be used by allowing the user to create acceptable certificates for those temporary keys. According to other (e.g. prior art) methods, such user-created certificates are not considered valid. In an embodiment of the present invention, user-created certificates are accepted, but they use the identity from a certificate already provided by a certificate authority (CA).

The present application also recognizes and solves a problem related to fraud. The solution of the present claimed invention is to place an appropriate temporal limit on the usage of the certificate. This temporal limit on usage is such that once a session on the other system is completed, then the certificate or a corresponding key is destroyed. The end of a session is the earliest practical point at which to destroy the certificate or key, without disrupting the session, and this insight has led Applicants to the present claimed invention.

#### **The Present Independent Claims Are Not Obvious From The Cited References**

Applicant respectfully submits that the present independent claims as amended are not obvious from *Seiichiro* in view of *Abburi*, or in further view of *Lauper*. Present claim 1 discloses that “once a session on the second system is completed, the certificate or a corresponding key is destroyed.” This session-completion limitation of present claim 1 is very different from what is disclosed in the new *Abburi* reference.

The Office Action asserts that this session-completion limitation of present claim 1 is disclosed by par. 0455, 0463-0469, 0461, and 0452 of *Abburi*. Applicant respectfully submits that this is incorrect.

Paragraph 0455 of *Abburi* only describes destroying a copy/replacement license (i.e. a license for a second system) when the original license expires (i.e. when the license for the first system expires). This is very different from present claim 1, which describes destroying a license for the second system when a session (e.g. a Secure Socket Layer session) on the second system expires.

Likewise, paragraph 0452 of *Abburi* discloses destroying a copy/replacement license for the second system when a fixed time has elapsed (e.g. two days). This fixed time period is completely unrelated to when a session on the second system is completed.

Likewise, paragraph 0461 of *Abburi* discloses destroying a copy/replacement license when thirty (30) days have elapsed since contacting a synchronization server. Again, this fixed time period is completely unrelated to when a session on the second system is completed.

Likewise, paragraphs 0463-0469 merely refers to the expiration schemes already described in *Abbur*i, none of which involve expiration when a session ends.

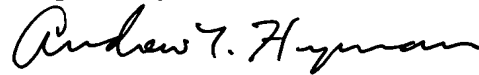
Because *Abbur*i nowhere suggests destroying a copy/replacement license once a session on the second system is completed, combining *Abbur*i with *Seiichiro* cannot yield the present claimed invention. These same arguments apply to the other independent claims as well. The cited combination of *Abbur*i with *Seiichiro* is thus far less effective at combating fraud as compared to the present claimed invention, which utilized the minimum practical amount of time for a copy/replacement license before that license is destroyed.

Application Serial No. 10/090,422  
Attorney Docket No. 944-005.002

**Conclusion**

It is therefore respectfully submitted that claims 1-57 and 60-67 are distinguished over the cited art and that the claims are therefore in condition for allowance. Such action is earnestly solicited.

Respectfully submitted,



Andrew T. Hyman  
Attorney for the Applicant  
Registration No. 45,858

ATH/mbh  
WARE, FRESSOLA, VAN DER SLUYS  
& ADOLPHSON LLP  
755 Main Street, PO Box 224  
Monroe CT 06468  
(203) 261-1234